UNITED STATES DISTRICT COURT
DISTRICT OF MARYLAND

LEADERS OF A BEAUTIFUL STRUGGLE *et al.*,

Plaintiffs,

v.

BALTIMORE POLICE DEPARTMENT *et al.*,

Defendants.

No. 20-cv-929-RDB

PLAINTIFFS' REPLY MEMORANDUM OF LAW IN FURTHER SUPPORT OF THEIR MOTION FOR A PRELIMINARY INJUNCTION

Brett Max Kaufman*
Ashley Gorski*
Alexia Ramirez*
Nathan Freed Wessler*
Ben Wizner*
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
T: 212.549.2500
F: 212.549.2654
bkaufman@aclu.org
agorski@aclu.org
aramirez@aclu.org
nwessler@aclu.org
bwizner@aclu.org

David R. Rocah (Bar No. 27315)
American Civil Liberties Union Foundation
of Maryland
3600 Clipper Mill Road, Suite 350
Baltimore, MD 21211
T: 410.889.8555
F: 410.366.7838
rocah@aclu-md.org

*pro hac vice

Counsel for Plaintiffs

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

INTRODUCTION

The BPD offers a handful of arguments in defense of the constitutionality of its wide-area aerial surveillance program, but none of them defeat Plaintiffs' showing that they are entitled to an injunction. The BPD contends that its surveillance is no different—less intrusive, even—than the aerial surveillance allowed by the Supreme Court in cases involving fleeting and targeted observations without advanced equipment. It argues that other Supreme Court cases have established that no one enjoys a reasonable expectation of privacy in any of their public movements. And it asserts that the Supreme Court's decision in *Carpenter v. United States*, 138 S. Ct. 2206 (2018), has nothing to say about those cases, or the BPD's system, either. None of that is correct. Indeed, it is not Plaintiffs' reading of *Carpenter* that is expansive—it is the BPD's program.

The BPD has also challenged Plaintiffs' standing under both the Fourth and First Amendments, but its ongoing, long-term apprehension of information about their whereabouts clearly suffices as an Article III injury. That injury will inflict irreparable harm on Plaintiffs, and the balance of equities and the public interest both favor Plaintiffs' requested injunction.

For the reasons laid out in Plaintiffs' earlier brief and those that follow, the Court should stop this program.

ARGUMENT

I. The BPD's wide-area aerial surveillance system goes far beyond the surveillance approved in decades-old Supreme Court cases, and it is unconstitutional.

The BPD rests the legal defense of its mass surveillance program on three pillars, none of which can bear the weight.

First, the BPD maintains that under several 1980s Supreme Court cases, "[a]erial photography and surveillance is not a search" under the Fourth Amendment. Defs.' Br. 12; *see*

id. at 12–14 (discussing *California v. Ciraolo*, 476 U.S. 207 (1986); *Dow Chemical Co. v. United States*, 476 U.S. 227 (1986); and *Florida v. Riley*, 488 U.S. 445 (1989)). Plaintiffs have already explained why those cases do not support the BPD's proposition, or bless its program: they involved targeted, transitory, short-term aerial observations of single targets with basic equipment or the naked eye. *See* Pls.' Br. 15–17. Still, the BPD insists that those cases "squarely" reach the widespread, persistent, long-term surveillance they intend to deploy over Baltimore. Defs.' Br. 14.

They don't. The BPD's surveillance is not "far less intrusive" than the surveillance in those cases. *Id*. It is true that the simple observations authorized in those cases included views of private or semi-private areas. But the same is true of the BPD's program, which will capture 90 percent of the city, including yards and curtilage. *See* Pls.' Br. 6, 16 n.46; *see also Ciraolo*, 476 U.S. at 214 (explaining that surveillance using "future electronic developments" would pose a far different case than a passing aerial observation from navigable airspace with the naked eye (quotation marks omitted)). Moreover, the BPD's claim that, unlike in those prior cases, it will not be engaging in surveillance of "specific, targeted, and identified individuals and/or properties" or "us[ing it] to track movements of specific individuals or vehicles," Defs.' Br. 14, is both false and beside the point. It is false because capturing such movements is the program's explicit goal and means of operation. *See* Pls.' Br. 6–9. And it is irrelevant because none of those cases involved tracking, over time, of anyone or anything at all; they dealt with fleeting observations of static geographic locations.

Second, the BPD suggests that the Supreme Court has endorsed a "general axiom" that "[o]bservation of public movements is not a search" under the Fourth Amendment. Defs.' Br. 14;

see id. at 14–16 (discussing *United States v. Jones*, 565 U.S. 400 (2012); *United States v. Knotts*, 460 U.S. 276 (1983)). But even before *Carpenter*, it wasn't so.

In *Knotts*, police warrantlessly tracked a criminal suspect's transport of a canister of a chemical used to make illicit drugs, using both visual surveillance and a beeper hidden inside the canister. *See* 460 U.S. at 278–79. In upholding the surveillance, the Court explained its view that "[a] person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another." *Id.* at 281. But that conclusion was explicitly and narrowly cabined—it applied only to movements "from one place to another," *id.*, during what the *Carpenter* Court later characterized as "a discrete 'automotive journey,'" 138 S. Ct. at 2215 (quoting *Knotts*, 460 U.S. at 285); *see id.* at 2220 ("[T]his case is not about 'using a phone' or a person's movement *at a particular time*." (emphasis added)). And the *Knotts* Court foresaw the problem addressed in *Jones* (and, later, *Carpenter*), warning that if law enforcement ever did manage, in the distant future, to implement "dragnet type law enforcement practices," there would be "time enough then to determine whether different constitutional principles" applied. 460 U.S. at 284.[1]

Thirty years later, in *Jones*, that time finally arrived—and the Court "found that different principles did indeed apply." *Carpenter*, 138 S. Ct. at 2215. While the *Jones* Court's majority opinion relied on a property-based theory to conclude that the police's use of a GPS device to track a vehicle for 28 days was a Fourth Amendment search, five Justices agreed in concurring opinions that longer-term location tracking "'impinges on expectations of privacy'—regardless whether those movements were disclosed to the public at large." *Id.* (quoting *Jones*, 565 U.S. at

[1] While Plaintiffs highlighted this critical observation from *Knotts*, *see* Pls.' Br. 14, the BPD's brief ignores it.

430 (op. of Alito, J., concurring), and citing *id.* at 415 (op. of Sotomayor, J., concurring)). So when the BPD insists that, "[i]n essence, the *Knotts* Court held that public visibility eliminates the reasonable expectation of privacy," or that "[t]he visibility of the object is dispositive as to whether a 'search' occurred," Defs.' Br. 15, it is overstating things considerably.

Third, the BPD argues that the logic of *Carpenter* does not reach its wide-area aerial surveillance program. *See id*. at 16–21. Again, it is wrong.

The BPD acknowledges that the *Carpenter* Court based its holding—that the government's warrantless acquisition of a compendium of cell-site location information was an unreasonable Fourth Amendment "search"—on its concern about "the breadth of the information the government could obtain about an individual's movement for a long period of time." *Id*. at 16. But the BPD still says its program is different.

For one, the BPD argues that the location information its program will collect about every Baltimorean is so fleeting that *Carpenter* doesn't reach it. *See id.* at 18. But that attempt to paper over the gravity of Defendants' proposed surveillance is not credible, either factually or legally. The BPD does not dispute that its cameras will capture a 45-day rolling log of all Baltimoreans' movements, and it acknowledges that its planes will scan the ground for 12 hours a day. *See id.* at 5, 18. While Defendants might prefer that this Court focus on the daily 12-hour window, the reality is that the BPD's planes will be aloft for more than 80 hours each week, weather permitting, and that the BPD will have 45 days' worth of aggregated data at a time. This time frame plainly exceeds the 7 days' worth of location information at issue in *Carpenter*.

While the program may not literally be round-the-clock surveillance, people do not reasonably expect constant monitoring during daylight hours with good weather, either.[2]

Of course, the record in *Carpenter* dictated the focus of its holding. There, two batches of location information were at issue—127 days obtained from one source, and seven days requested from another.[3] *See* 138 S. Ct. at 2217 & n.3. In holding that collecting seven days of location data is a search, the Court did not hold, or even suggest, that collection of location data over a shorter period shorter would evade Fourth Amendment protection. Indeed, multiple courts, before and after *Carpenter*, have held that much shorter collections of location information deserve protection. *See, e.g.*, *State v. Muhammad*, 451 P.3d 1060, 1072–73 (Wash. 2019) (holding that a single ping of cell-phone location information is a Fourth Amendment search requiring a warrant); *Commonwealth v. Almonor*, 120 N.E.3d 1183, 1197 (Mass. 2019) (same); *see also, e.g.*, *Commonwealth v. Estabrook*, 38 N.E.3d 231, 237 & n.11 (Mass. 2015) (holding, pre-*Carpenter*, that police could acquire up to only six hours of historical cell-site location information without triggering a search under the state analogue to the Fourth Amendment).[4] Those rulings make sense. As Justice Sotomayor pointed out in *Jones*, "even

---

[2] There is at least some factual question whether the BPD's planes will end up flying more than 12 hours per day, including at night. Ross McNutt, the President of Persistent Surveillance Systems, suggests as much. *See* Defs.' Br. 3 (citing Declaration of Ross T. McNutt, PhD. ("McNut Decl.") ¶ 5 (attached as Exhibit A to Defs.' Br.)). But that is not a limitation in the BPD's contract, which does include a representation that the BPD's cameras are "sensitive enough to capture images at night with ambient City lighting." BPD/PSS Contract at 19.

[3] *But see Carpenter*,138 S. Ct. at 2266–67 (Gorsuch, J., dissenting) (pointing out that the government only actually received, and viewed, two days of the defendant's location information from the second source).

[4] The BPD has argued that it is relevant that under the contract, the BPD's surveillance system is not authorized to engage in real-time surveillance, or even capable of doing so. *See* Defs.' Br. 4. But the *Carpenter* Court emphasized that the use of location tracking to amass reams of historical data is especially problematic, because its function is to generate "retrospective" data

short-term monitoring" of location using advanced technologies implicates society's reasonable expectations of privacy by threatening to reveal "a wealth of detail about . . . familial, political, professional, religious, and sexual associations" and thereby "alter[ing] the relationship between citizen and government in a way that is inimical to democratic society." 565 U.S. at 415–16 (Sotomayor, J., concurring).

As a result, the BPD's arguments that "shorter collection" (by which it means 12 hours straight, with each block of time considered separately) "is permissible," Defs.' Br. 18, and that its program "will not, indeed cannot, capture continuous activities of individuals," *id.* at 20 (citing McNutt Decl. ¶ 14), are, constitutionally speaking, beside the point. As are the pre-*Carpenter* cases holding that weeks of different types of surveillance were permissible. *See id.* at 18–19. In *Carpenter*, the government made the same argument, using the same cases. *See* Br. of United States at *56–57, *United States v. Carpenter* (No. 16-402), 2017 WL 4311113 (Sept. 25, 2017). The Court was not persuaded.[5]

---

that can be indefinitely mined by law enforcement—granting it access to a virtual time machine. 138 S. Ct. at 2218.

[5] Only one of the cases the BPD cites actually involved anything close to longer-term, round-the-clock surveillance; and even there, it is impossible to tell from the opinion in the case the extent to which the suspect was continuously tailed. *See United States v. Gramlich*, 551 F.2d 1359 (5th Cir. 1977). The BPD's other examples involved surveillance of one or more stationary locations—an exercise that is far less invasive and resource-intensive than tailing a suspect on the move. *See Young v. Owens*, 577 F. App'x 410, 412 (6th Cir. 2014) (store); *United States v. Gaskins*, 690 F.3d 569, 574 (D.C. Cir. 2012) (multiple static locations); *United States v. Johnson*, 480 F. App'x 835, 837 (6th Cir. 2012) (residence). And, as Plaintiffs have noted, the logic of cases approving extended surveillance of single locations, through pole cameras or otherwise, has been cast into serious doubt by *Carpenter*. *See* Pls.' Br. 16 n.46 (citing *United States v. Moore-Bush*, 381 F. Supp. 3d 139, 149 (D. Mass. 2019) (holding that a "home occupant would not reasonably expect" eight months of surveillance with a pole camera); *see also Carpenter*, 138 S. Ct. at 2219 ("Unlike the nosy neighbor who keeps an eye on comings and goings, [advanced surveillance technologies] are ever alert, and their memory is nearly infallible.").

The BPD also insists that its program is untouched by *Carpenter* because it captures only "dots," Defs.' Br. 1—by which it means people—which are not identifiable in a way the Fourth Amendment cares about. As Plaintiffs have pointed out, the *Carpenter* Court rejected a similar argument. *See* Pls.' Br. 18. Unlike the information the BPD plans to log, the location information at issue in *Carpenter* was blunt, rather than precise, requiring analysts to draw inferences about a suspect's precise location and activities. *See id.* at 13 n.43. Nor was the information in *Carpenter* automatically associated with an identifiable person; instead, it was tied to a phone number. The fact that an analyst may need to consult other sources of information to derive a person's identity is not an investigatory step that "insulates" a search under the Fourth Amendment. *Carpenter*, 138 S. Ct. at 2218 (quoting *Kyllo v. United States*, 533 U.S. 27, 36 (2001)); *see* Pls.' Br. 18.[6] And besides, the Supreme Court has now made repeatedly clear that courts evaluating the uses of surveillance technologies against the Fourth Amendment cannot close their eyes to technological developments that will render those capabilities quaint. *See id.* at 2218 (citing *Kyllo*, 533 U.S. at 34–36). As Plaintiffs have pointed out, more advanced technologies are already available from the BPD's private partner in this surveillance program, and are just a tweak of contractual language away from becoming reality. *See* Pls.' Br. 18–19.

Relatedly, the BPD argues that its program will not create an "easily prepared individually identifiable record," Defs.' Br. 18, and that it will not be "possible to stitch imagery together to track the same subject day after day," *id*. at 4–5 (citing McNutt Decl. ¶ 14). In order to do that, it says, analysts would have to spend hours analyzing footage. But even if this process

[6] *See also* Pls.' Br. 17–18 (discussing study finding that just four location points can be used to specifically identify 95 percent of individuals).

is—for now, at least, given the rapid spread of video analytics software[7]—somewhat more resource-intensive than what was at issue in *Carpenter*, that process was not automated, either; law enforcement could not simply pull up a Google Map of the suspects' whereabouts using cell-site location information alone. *See United States v. Carpenter*, 819 F.3d 880, 885 (6th Cir. 2016) (describing investigator's steps to render location records meaningful). Moreover, as the BPD's contract describes, a central purpose of its wide-area aerial surveillance is to enable identification through the use of its other surveillance technologies, like automatic license-plate readers and ground security cameras. *See* Pls.' Br. 7–8, 18. And, of course, people who return home at night and leave again in the morning will have put—by virtue of simply existing in the day-to-day grind—their specific movements at the BPD's fingertips.

The BPD's other attempts to cast *Carpenter* aside also fail. The BPD argues that its surveillance will not capture Baltimoreans' movement inside private spaces, *see* Defs.' Br. 17–18—but while certain Supreme Court cases have highlighted the Fourth Amendment's heightened protections inside the home, *see, e.g.*, *United States v. Karo*, 468 U.S. 705 (1984) (not cited at all in *Carpenter*), the *Carpenter* Court was focused not on private but *public* space, and "a person's expectation of privacy in his physical location and movements" generally. 138 S. Ct. at 2215.[8] Next, the BPD maintains that the location information at issue in *Carpenter* was

[7] *See* Jay Stanley, ACLU, The Dawn of Robot Surveillance: AI, Video Analytics, and Privacy (June 2019), https://www.aclu.org/sites/default/files/field_document/061119-robot_surveillance.pdf (describing how video analytics capabilities can be used, among other things, to automatically alert authorities based on often-unexplainable algorithmic decision making).

[8] The BPD's argument on this point also ignores that its surveillance system will undoubtedly track activities inside of private yards or other areas of curtilage protected by the Fourth Amendment, in addition to Baltimoreans' movements *to* such private spaces. *See* Pls.' Br. 16 n.46; *see also Karo*, 468 U.S. at 716 ("We cannot accept the Government's contention that it should be completely free from the constraints of the Fourth Amendment to determine by means of an electronic device, without a warrant and without probable cause or reasonable suspicion,

"unique[]" because cell phones are "omnipresent." Defs.' Br. 17. But the *Carpenter* Court's observation that the use of a cell phone is so "indispensable to participation in modern society," 138 S. Ct. at 2220, applies with even greater force to the ability to simply move about in public. *See* Pls.' Br. 13.

And the BPD's argument that it, as opposed to its private partner, only receives some data, rather than the entire 45-day log, is immaterial twice over. First, the initial collection of this information is "state action" attributable to Defendants under 42 U.S.C. § 1983, *see* Pls.' Br. 11 n.41, a point the BPD does not expressly dispute. And second, the procedures that govern how the BPD receives and handles location information are not relevant to whether a "search" has occurred, but only to whether that search is reasonable under the Fourth Amendment.[9] (As Plaintiffs have explained, the AIR program's collection is not. *See id*. at 19–28.[10])

---

whether a particular article—or a person, for that matter—is *in* an individual's home at a particular time." (emphases added)).

[9] Curiously, Mr. McNutt claims in his declaration that the ACLU, one of the organizations representing Plaintiffs in this case, has provided "input" that factored into the privacy policies reflected in the BPD's contract. *See* McNutt Decl. ¶ 18. That is a claim Mr. McNutt has been making for years, and it is simply untrue. *See* Jay Stanley, *Baltimore Aerial Surveillance Program Retained Data Despite 45-Day Privacy Policy Limit*, ACLU Free Future Blog (Oct. 25, 2016), https://www.aclu.org/blog/free-future/baltimore-aerial-surveillance-program-retained-data-despite-45-day-privacy-policy (explaining that Mr. McNutt's claim that the "State and National ACLU" helped "develop" his privacy policies "could [not] be further from the truth"). As the ACLU's Mr. Stanley writes, "McNutt asked to meet with me, I agreed, and told him what I thought the insoluble privacy problems were with wide-area surveillance. He may have taken account of my feedback in formulating his policy, and we can't stop him from citing that feedback in its formation, but nobody should think that we are okay with this approach to law enforcement." *Id*.

[10] The BPD does not argue that its warrantless wide-area aerial surveillance program should be analyzed under the special-needs doctrine. *See* Pls. Br. 19–24. As a result, the program is per se unconstitutional if the Court agrees that the bulk collection of Baltimoreans' location information is a Fourth Amendment "search."

While the BPD floats the possibility that it might, after all, end up asking for warrants before accessing some of its evidence packages as part of this program, *see* Defs.' Br. 23, it does so notwithstanding the absence of a single contract term or prior public assurance to that effect.

Finally, the BPD effectively says privacy in public is already a dead letter in Baltimore City. *See* Defs.' Br. 21. Plaintiffs dispute that. *See, e.g.*, LBS Decl. ¶¶ 10–16; Bridgeford Decl. ¶¶ 10–16; James Decl. ¶¶ 5–8. Moreover, the *Carpenter* Court understood that other surveillance of public space was in effect, yet it still ruled as it did. In any event, the Fourth Amendment's protections cannot be breezily cast aside by claiming that an onslaught of privacy invasions renders public expectations of privacy inert.[11]

In the end, though the BPD likens its program to surveillance that law enforcement was routinely conducting forty years ago, its system is far different from anything that has ever come before. And it is hardly an "expansive[]" reach, Defs.' Br. 16, to understand the Supreme Court's digital-privacy decisions over the past decade as forming a bulwark against precisely this type of comprehensive mass surveillance system. Just as Chief Justice Roberts warned in *Carpenter*, this kind of surveillance "gives police access to a category of information otherwise unknowable." 138 S. Ct. at 2218. Far from providing a mere "technological assist," Defs.' Br. 16, it removes practical checks that have ensured Fourth Amendment protection of individual privacy since the Founding, and would open the door to "a too permeating police surveillance." *Carpenter*, 138 S. Ct. at 2214 (quotation marks omitted). That is why the BPD is wrong to suggest that "[i]f it would be constitutionally permissible for a law enforcement officer to surveil an individual during daylight hours on foot, then it must too be constitutional for the officer to do so using the AIR program." Br. 16. The BPD's system does not track just one person; it tracks everyone,

[11] *Cf. Smith v. Maryland*, 442 U.S. 735, 740 n.5 (1979) ("For example, if the Government were suddenly to announce on nationwide television that all homes henceforth would be subject to warrantless entry, individuals thereafter might not in fact entertain any actual expectation [of] privacy regarding their homes, papers, and effects. . . . [But i]n such circumstances, where an individual's subjective expectations had been 'conditioned' by influences alien to well-recognized Fourth Amendment freedoms, those subjective expectations obviously could play no meaningful role in ascertaining what the scope of Fourth Amendment protection was.").

efficiently and comprehensively. *See Commonwealth v. McCarthy*, No. SJC-12750, 2020 WL 1889007, at *5 (Mass. Apr. 16, 2020) (approving of limited surveillance by automatic license-plate readers, but warning that "we imagine Massachusetts residents would object were the police continuously to track every person's public movements by traditional surveillance methods, absent any suspicion at all").

The public can decide for itself whether the BPD's surveillance system is sufficiently "dystopian" or "Orwellian" to earn those labels, or not. Defs.' Br. 16, 9. What matters here, and to this Court, is that it is prohibited by the Fourth Amendment.

II. Plaintiffs have standing to challenge the BPD's collection of their location information.

A. Plaintiffs have standing to raise their Fourth Amendment claim.

The BPD argues that Plaintiffs lack standing to bring their Fourth Amendment claim because "they have not shown that data capturing their individual movements will be reviewed by BPD, or that BPD would have any way of identifying them specifically." Defs.' Br. 22. Plaintiffs have already addressed the latter argument above. As to the former, the BPD ignores Plaintiffs' central Fourth Amendment claim: the collection of Plaintiffs' location data is a Fourth Amendment "search." It is also a distinct Article III injury, regardless of whether this Court determines that the collection violates the Fourth Amendment on the merits. *See, e.g.*, *ACLU v. Clapper*, 785 F.3d 787, 801–03 (2d Cir. 2015) (holding that plaintiffs had standing under Fourth and First Amendment to challenge the National Security Agency's bulk collection of telephone records, even absent subsequent government review of those records).

Moreover, that the BPD's private partner will initially collect this data is not important, as that collection will plainly be attributable to the BPD under Section 1983. *See* Pls.' Br. 11 n.40. The AIR program involves the explicit delegation and direction of policing functions to

PSS through a contract signed by a final policymaker—the Baltimore Police Commissioner. *See id.* (citing cases). As a result, there is an incredibly "close nexus" between PSS and the BPD, and PSS is "exercis[ing] powers that are traditionally the exclusive prerogative of the state." *Conner v. Donnelly*, 42 F.3d 220, 224 (4th Cir. 1994) (quotation marks omitted); *see also Blum v. Yaretsky*, 457 U.S. 991, 1003–05 (1982) (explaining that the state can be held "responsible for a private decision" where it has provided "significant encouragement" to the private actor). The BPD has made no argument to the contrary. Accordingly, PSS's activities through the AIR program are attributable to Defendants and constitute state action under Section 1983.

The BPD also errs in contending that *Carpenter* helps its standing argument because "the Court did not prohibit the cell phone providers from collecting CSLI." Defs.' Br. at 22. The cell phone providers in *Carpenter* were not operating as extensions of the government; they had not signed contracts through which the government directed them to collect all cell phone users' location information. Indeed, that made *Carpenter* a much more difficult case than this one.

B. Plaintiffs have standing to raise their First Amendment claim.

The BPD does not dispute the merits of Plaintiffs' First Amendment claim, effectively conceding the likelihood of its success. *See* Defs.' Br. 23–27. Rather, the BPD's only argument is that Plaintiffs lack standing to challenge the AIR program's violation of their First Amendment rights. The BPD is mistaken.

To establish standing to redress harm under the First Amendment, a plaintiff must show the ordinary elements required by Article III: injury-in-fact, a sufficient causal connection between the injury and the conduct complained of, and a likelihood that the injury will be redressed by a favorable decision. *See Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 157–58 (2014). But several circuits, including the Fourth, have "held that 'standing requirements are

somewhat relaxed in First Amendment cases,' particularly regarding the injury-in-fact requirement." *Davison v. Randall*, 912 F.3d 666, 678 (4th Cir. 2019) (quoting *Cooksey v. Futrell*, 721 F.3d 226, 235 (4th Cir. 2013)). The sole dispute here is whether Plaintiffs are likely to succeed in establishing injury-in-fact to support their First Amendment claim. For the reasons below, it is plain that Plaintiffs have established cognizable injuries.

First, by collecting information about virtually all of Plaintiffs' associations through the AIR program, the BPD's program will impair Plaintiffs' First Amendment rights. This collection of sensitive information is an injury sufficient to establish standing. *See, e.g.*, *ACLU v. Clapper*, 785 F.3d at 802 (holding that the government's mass collection of plaintiffs' metadata implicated their "interests in keeping their associations and contacts private," thus conferring standing to assert a First Amendment violation). In the course of their work and daily lives, Plaintiffs meet with myriad groups and individuals, and many of these associations are private and sensitive. LBS Decl. ¶ 13; Bridgeford Decl. ¶¶ 12, 15; James Decl. ¶ 8. The AIR program substantially impairs Plaintiffs' First Amendment rights because it exposes virtually all of their associations to government monitoring and scrutiny.

Second, if the AIR program is allowed to proceed, Plaintiffs will be forced to take several measures to protect the privacy of their associations from the BPD's surveillance. For example, LBS will "alter[] the means by which [they] travel" and the "timing of certain meetings," thus diverting resources from other organizational work. LBS Decl. ¶ 13. Similarly, Ms. Bridgeford will "shift most of [her] outreach and conversations to be over the phone, over social media, or over email, which will severely impact the nature and quality of the inherently personal and sensitive work" that she does through Ceasefire. Bridgeford Decl. ¶ 15. It is well-established that these harms confer standing. *See, e.g.*, *Dep't of Commerce v. New York*, 139 S. Ct. 2551, 2565

(2019) (recognizing that an organization's "diversion of resources" in response to a defendant's actions is an injury-in-fact sufficient for standing); *Wikimedia Found. v. NSA*, 857 F.3d 193, 211 (4th Cir. 2017) (holding that where an organization alters its means of communication in response to the threat of surveillance, it suffers a First Amendment injury).

Citing *Clapper v. Amnesty International USA*, 568 U.S. 398 (2013), the BPD contends that protective measures taken in response to fear of surveillance are "categorically insufficient" to establish standing for a First Amendment claim. Defs.' Br. 26. But *Amnesty* stands for no such thing. In fact, in *Amnesty*, the Supreme Court expressly recognized that a plaintiff may establish standing by showing that it took protective measures to mitigate the harms of government surveillance. *See* 568 U.S. at 414 n.5. Although the plaintiffs in *Amnesty* had taken such steps, the Court concluded that their measures were insufficient because the risk of surveillance there was an entirely "hypothetical future harm." *Id.* at 401. Here, unlike in *Amnesty*, the AIR program's mass collection is in no way "hypothetical"—it is, in fact, imminent—and it is undisputed that Plaintiffs will be subject to it. Accordingly, Plaintiffs' protective measures are sufficient to establish standing for their First Amendment claim. *See id.* at 414 n.5; *Monsanto Co. v. Geertson Seed Farms*, 561 U.S. 139, 154–55 (2010).[12]

Third, the BPD's program will chill Plaintiffs and the individuals they associate with, burdening Plaintiffs' political advocacy and community engagement. LBS Decl. ¶¶ 12–16; Bridgeford Decl. ¶¶ 11–13, 15–16; James Decl. ¶¶ 5–8. Defendants assert that chilling effects cannot serve as a basis for Plaintiffs' standing, Defs.' Br. 25, but that is incorrect, *see, e.g.*, *Wikimedia*, 857 F.3d at 211 (citing *ACLU v. Clapper*, 785 F.3d at 802) (recognizing that where

[12] Moreover, Plaintiffs Bridgeford and James have established a substantial risk that the AIR program will develop individualized reports on them and their activities. *See* Bridgeford Decl. ¶ 10; James Decl. ¶ 6.

the government collects a plaintiff's information, a "chilling effect" is created at that point, providing a basis for First Amendment standing); *see also, e.g.*, *Local 1814, Int'l Longshoremen's Ass'n, AFL-CIO v. Waterfront Comm'n of N.Y. Harbor*, 667 F.2d 267, 270–72 (2d Cir. 1981) (recognizing that the government's collection of information about associational information results in First Amendment chill).

Contrary to the BPD's claim, Defs.' Br. 25, Plaintiffs' specific allegations of chill are nothing like the allegations rejected by the Court in *Laird v. Tatum*, 408 U.S. 1 (1972), in which the plaintiffs challenged an Army surveillance program on First Amendment grounds. In *Laird*, the plaintiffs alleged that they were "chilled by the mere existence, *without more*, of a governmental investigative and data-gathering activity." *Id.* at 10 (emphasis added). Notably, the plaintiffs presented "no evidence of illegal or unlawful surveillance activities," *id.* at 9 (quoting *Tatum v. Laird*, 444 F.2d 947, 953 (D.C. Cir. 1971))—presumably because the "principal sources of information" for this surveillance program were "the news media and publications in general circulation," *id.* at 6. The plaintiffs also failed to explain the "precise connection between the mere existence of the challenged system and their own alleged chill," and "cast considerable doubt on whether they themselves are in fact suffering from any such chill." *Id.* at 13 n.7. In holding that the plaintiffs had failed to establish standing, the *Laird* Court emphasized that its conclusion was "a narrow one," based on the record before it. *Id.* at 15.

Unlike the plaintiffs in *Laird*, Plaintiffs here have not merely alleged that the BPD's program chills their First Amendment rights; rather, they have presented extensive "evidence of illegal or unlawful surveillance activities." *Id.* at 9; *see supra* Part I; *see also Hassan v. City of New York*, 804 F.3d 277, 292 (3d Cir. 2015) (holding that *Laird* was inapplicable where plaintiffs challenged surveillance on both due process and First Amendment grounds). Moreover,

the harms to Plaintiffs here flow from more than the "mere existence" of the AIR program, *Laird*, 408 U.S. at 10; they flow from the certainty that Plaintiffs and their associations will in fact be subject to this comprehensive surveillance, *see Amnesty*, 568 U.S. at 417 n.7. Unlike in *Laird*, Plaintiffs have explained why the government's collection of information about them and their associations is imminent, and why this collection will objectively chill and burden their First Amendment activity. LBS Decl. ¶¶ 12–16; Bridgeford Decl. ¶¶ 10–16; James Decl. ¶¶ 5–8. This chill is due in part to the breadth and intrusiveness of the BPD's program, which goes far beyond the Army's targeted collection of news articles. *Laird*, 408 U.S. at 6.[13]

The BPD's reliance on *Donohoe v. Duling*, 465 F.2d 196 (4th Cir. 1972), is similarly misplaced. *See* Defs.' Br. 26. In *Donohoe*, as in *Laird*, the plaintiffs claimed that the exercise of their First Amendment rights was "chilled by the mere existence, without more," of a government surveillance activity. 465 F.2d at 202 (quoting *Laird*, 408 U.S. at 10). Moreover, the defendants in *Donohoe* "denied that any of the plaintiffs had been inhibited in the exercise of their First Amendment rights by any action on their part; and no plaintiff testified to the contrary." *Id.* at 199. Here, in contrast, Plaintiffs have attested to concrete and specific First Amendment injuries flowing from the BPD's program. The BPD has not denied the existence of these injuries or their traceability to the program; it has only challenged their legal sufficiency. *See* Defs.' Br. 23–27. For the reasons above, the law is clear that these injuries—the program's collection of Plaintiffs' private associational information, the Plaintiffs' protective measures, and the concrete chilling effects—are each plainly sufficient to establish Plaintiffs' standing.

[13] Defendants also err in suggesting that Plaintiffs must establish that their chill is the result of "regulat[ion]" by the BPD. Defs.' Br. 24. No such requirement exists. *See Wikimedia*, 857 F.3d at 211 (holding that a plaintiff challenging government surveillance—which did not involve direct regulation of the plaintiff—adequately alleged First Amendment chill).

III. Plaintiffs will suffer irreparable harm as a result of the BPD's wide-area aerial surveillance system, and the balance of equities and public interest weigh in their favor.

The BPD is also wrong when it argues that Plaintiffs are not entitled to an injunction of the BPD's program.

First, if permitted to proceed, the BPD's AIR program will cause irreparable harm to Plaintiffs. The BPD's system and collection of images amounts to continuous, warrantless mass surveillance, which violates Plaintiffs' Fourth and First Amendment rights. *See supra* Parts I–II. This violation of constitutional rights establishes manifest, irreparable harm. *See WV Ass'n of Club Owners & Fraternal Servs., Inc. v. Musgrave*, 553 F.3d 292, 298 (4th Cir. 2009); *Mills v. District of Columbia*, 571 F.3d 1304, 1312 (D.C. Cir. 2009).

Second, the balance of equities weighs heavily in favor of an injunction. Plaintiffs will suffer significant, irreparable harm in the absence of an injunction as the BPD compiles video of their daily movements. The BPD, on the other hand, faces little if any injury from its issuance. The BPD claims that it will be injured by the *possibility* that the "window of this opportunity" to test the AIR Program with philanthropic support may close. Defs.' Br. 30. The assertion that funding will not be available for the BPD's wide-area aerial surveillance program after this Court has had the opportunity to evaluate the Program's constitutionality is entirely speculative, and it is not supported by any evidence in the record.[14] Furthermore, even if that claim proves true, the loss of the ability to test a likely unconstitutional program does not tip the balance of equities in

[14] The BPD also argues that data collected while Baltimoreans are under orders to stay at home, due to the COVID-19 pandemic, will meaningfully inform its decision whether to make the AIR program a permanent part of city life because crime has continued despite those orders. *See* Defs.' Br. 6 n.6. But that argument conflates a hypothetical showing that the program reduced crime during a period of social distancing with a showing that the program reduces crime in ordinary social circumstances. *See* Pls.' Br. 34.

Defendants' favor. The Fourth Circuit has recognized that government officials are not harmed by the issuance of a preliminary injunction that prevents the state from implementing a likely unconstitutional practice. *See Centro Tepeyac v. Montgomery Cty.*, 722 F.3d 184, 191 (4th Cir. 2013) (quoting *Giovani Carandola, Ltd. v. Bason*, 303 F.3d 507, 521 (4th Cir. 2002)); *see also Rodriguez v. Robbins*, 715 F.3d 1127, 1145 (9th Cir. 2013).

Finally, preliminarily enjoining the BPD's wide-area aerial surveillance program is manifestly in the public interest. Defendants have characterized this final factor as an inquiry into which party has more accurately understood the wishes of the Baltimore community. However, as Defendants concede, "[t]he injunctive relief analysis is not a popularity contest." Defs.' Br. 29. The public-interest inquiry is not about whether the majority of Baltimoreans favor the BPD's wide-area aerial surveillance program. Instead, it is about whether the public interest favors granting preliminary injunctive relief until this Court can rule on the constitutionality of the BPD's aerial surveillance system. It is undeniably in the public's interest to have their constitutional rights protected. *See Bason*, 303 F.3d at 521 (finding that "upholding constitutional rights surely serves the public interest").

CONCLUSION

For the foregoing reasons and those in Plaintiffs' prior memorandum, this Court should enjoin Defendants' AIR program—specifically, by prohibiting the BPD from collecting or accessing any images of Baltimoreans through wide-area aerial surveillance.

April 17, 2020

Respectfully submitted,

/s/ David R. Rocah

David R. Rocah (Bar No. 27315)
American Civil Liberties Union Foundation
of Maryland
3600 Clipper Mill Road, Suite 350
Baltimore, MD 21211
T: 410.889.8555
F: 410.366.7838
rocah@aclu-md.org

Counsel for Plaintiffs

Brett Max Kaufman*
Ashley Gorski*
Alexia Ramirez*
Nathan Freed Wessler*
Ben Wizner*
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
T: 212.549.2500
F: 212.549.2654
bkaufman@aclu.org
agorski@aclu.org
aramirez@aclu.org
nwessler@aclu.org
bwizner@aclu.org

**pro hac vice*

CERTIFICATE OF SERVICE

I hereby certify that on the 17th day of April, 2020, I electronically filed the foregoing Plaintiffs' Reply Memorandum in Support of Their Motion for a Preliminary Injunction with the clerk of the Court by using the CM/ECF system, which will send a notice of electronic filing.

/s/ *David R. Rocah*
David R. Rocah (Bar No. 27315)
American Civil Liberties Union Foundation
of Maryland
3600 Clipper Mill Road, Suite 350
Baltimore, MD 21211
T: 410.889.8555
F: 410.366.7838
rocah@aclu-md.org